UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/574,909	04/06/2006	**Vincent Carlier**	4005-0277PUS1	7126

77032 7590 01/05/2010

Joe McKinney Muncy
PO Box 1364
Fairfax, VA 22038-1364

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	PAPER NUMBER
2439	
MAIL DATE	DELIVERY MODE
01/05/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 10/574,909
Filing Date: April 06, 2006
Appellant(s): CARLIER ET AL.

Joe McKinney Muncy (Reg. No. 32,334)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 09 October 2009 appealing from the Office action mailed 11 May 2009.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

4,922,539	RAJASEKARAN	05-1990
2004/0187035	SCHWAN et al.	09-2004

Schneier, Bruce "Applied Cryptography, Protocol, Algorithms, and Source Code in C" 1996, pp. 270-285.

Stallings, William. "Cryptography and Network Security: Principles and Practices" Prentice Hall, 3rd Ed. (2003), pp. 56-98.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-4 and 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 2004/0187035 A1 to Schwan et al., hereinafter Schwann, in view of known techniques.

As per claims 1 and 6, factoring is a technique taught to simplify complex polynomial equations. Factoring polynomials into quadratics, or simpler equations of at least a second degree (i.e. x^2), is known. U.S. Patent No. 4,922,539 to Rajasekaran et al., hereinafter Rajasekaran, discloses using the Bairstow technique for factoring polynomials with real coefficients into a set of quadratic polynomials for speech recognition (column 5, line 58 to column 6, line 14). The Applicant claims factoring a cryptographic equation in order to protect said equation prior to being implemented on a computer. MPEP 2112(I) states that the claiming of a new use, new function, or unknown property which is inherently present in the prior art does not necessarily make the claim patentable. See also *In re Best*, 562 F.2d 1252, 1254, 195 USPQ 430, 433 (CCPA 1977). In other words, the fact that the Applicant has found that factoring can be used to protect a cryptographic equation does not make the claim patentably distinct since factoring of complex polynomials has been well-known and commonly practiced in at least the field of speech recognition since 1990. Recombining equations to form polynomials is also well-known and commonly practiced. This technique is typically taught in high school algebra on a much more basic level, such as $5(x - 1)(x + 2)(x - 3)(x + 4) = 5x^4 + 10x^3 - 65x^2 -70x + 120$. One of ordinary skill would clearly be able to recombine several quadratic equations to reform the original polynomial. As noted in the previous Office Actions, Schwann teaches implementing an cryptographic algorithm n a processor (paragraphs 0002, 0010, 0015).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the known techniques of factoring a complex polynomial, recombining said quadratics that were factored, and using said complex polynomial to introduce an encryption algorithm to a device, since it has been held that it only requires routine skill in the art to combine known elements to yield a predictable result. See MPEP § 2141(III); see also *KSR International Co. v. Teleflex Inc.*, 550 USPQ2d 1385 (2007).

Regarding claims 2 and 7, Schwan teaches the step of storing the encryption algorithms in the form of a configuration file that is loaded into a memory associated with the processor unit (paragraph 0002, i.e. updating the control program, programming the control unit to a customer and application needs, modify the functional and performance range of the control unit, reprogramming the control unit).

With regards to claims 3 and 8, Schwan teaches wherein the memory and the programmable processor unit are associated with an eraser member serving, in the event of an intrusion into the device, to erase the processor unit, and to erase the memory containing the configuration file when the configuration is present in said memory (paragraph 0013, i.e. encryption algorithm is erased and/or destroyed after the housing is opened (the intrusion)).

Regarding claims 4 and 9, Schwan discloses the use of DES (paragraph 0013). As noted above DES combines more than two initial polynomials in order to obtain combined polynomials. DES also includes a function f_k and f_k^{-1}. This is supported by the disclosure of DES in **Cryptography and Network Security, Principles and Practices**, by William Stallings, hereinafter Stallings. Specifically, Stallings discloses the function f_k on at least page 61, or the initial permutation as disclosed on page 57. Stallings goes on further to discuss on page 57 the inverse initial permutation towards the end of the cryptographic calculation. Therefore Schwan teaches the step of combining each combined polynomial (Q_k) with a function (f_k), and of combining the following combined polynomial (Q_{k+1}) with an inverse function (f_k^{-1}) in his disclosure of DES.

Claims 5 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schwan in view of known techniques as applied above and in further view of **Applied Cryptography, Protocols, Algorithms, and Source Code in C**, by Bruce Schneier, hereinafter Schneier.

With regards to claims 5 and 10, Schwan does not teach wherein the function (f_k) combined with each combined polynomial (Q_k) is a linear function.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the initial permutation, or claimed function f_k, be a linear function, since Schneier states at page 271 that the initial permutation is used to transpose the input block of data, and as such a linear function would make it easier to transpose the input block and load the plaintext and ciphertext into a DES chip in byte-sized pieces.

(10) Response to Argument

Appellant's arguments filed 09 October 2009 have been fully considered but they are not persuasive. The Appellant argues, with respect to independent claims 1 and 6, that the prior art does not teach "protecting a cryptographic algorithm before introduction in a device."

First, the recitation "protecting a cryptographic algorithm before introduction in a device" has not been given much patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

In addition, appellant's argument that the prior art does not disclose "protecting a cryptographic algorithm before introduction in a device" amounts to a recitation of the intended use of the claimed invention. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.

Assuming that patentable weight should be given to the appellant's arguments that the prior art does not teach "protecting a cryptographic algorithm before introduction in a device," the examiner turns to the limitations set forth to accomplish this purpose. The independent claims require that a cryptographic algorithm be separable into initial polynomials of at least two variables each, and having a degree of not less than two; these at least two quadratic equations are provided to the enciphering device where they are combined and run to encrypt data.

The examiner has interpreted the separating of the cryptographic algorithm into initial polynomials of at least two variables each, and having a degree of not less than two, as factoring. Factoring is a technique for decomposing an object, such as a polynomial, into a product of other objects. The examiner relies upon U.S. Patent No. 4,922,539 to Rajasekaran et al. to disclose one technique, namely the Bairstow technique, for factoring polynomials with real coefficients into a set of quadratic polynomials (column 5, line 58 to column 6, line 14). While Rajasekaran factors the polynomials for speech recognition, factoring polynomials into sets of quadratic polynomials is well-known and commonly practiced regardless of any new uses the appellant has found its application. The claiming of a new use, new function, or unknown property which is inherently present in the prior art does not necessarily make the claim patentable. MPEP § 2112(I). See also *In re Best*, 562 F.2d 1252, 1254, 195 USPQ 430, 433 (CCPA 1977). In other words, the fact that the appellant has found that factoring can be used to protect a cryptographic equation does not make the claim patentably distinct since factoring of complex polynomials has been well-known and commonly practiced in at least the field of speech recognition since 1990.

The next claimed step is providing the enciphering device at least two initial polynomials. The examiner takes the position that providing information to a computer is inherent to computer systems. First, with regards to providing the enciphering device at least two initial polynomials, the examiner asserts that computers need to have information installed in order for them to perform the processes desired by the user. Computers do not come with Microsoft Word or Excel or even Windows; if a user wishes to have the operability of those applications, she must provide or install them on the computing device. Paragraph 0015 of U.S. Patent Application Publication No. 2004/0187035 A1 to Schwan et al. disclose a number of encryption algorithms that were provided to a computing device. Although Schwan is silent on how the encryption algorithms arrived on the computing device, one of ordinary skill in the art would recognize that someone had to provide them. Therefore, one of ordinary skill in the art would at least know how to provide two data sets, such as quadratic polynomials of a cryptographic equation, to a computing device.

The next limitation is combining, on the enciphering device, combined polynomials each obtained from the at least two initial polynomials. Again, the examiner takes the position that this step is inherent. The earliest computing devices were calculators, and even today computers perform millions of calculations a second. It would not take a computer much computing power to combine two quadratic polynomials, a skill taught in American schools no later than sixth grade. Furthermore, Schwan discloses combining data in paragraph 0015 in stating that "keys are generated on the basis of two large prime numbers." Therefore, one of ordinary skill in the art would know how to combine polynomials.

The last limitation is implementing the combined polynomials in the programmable processor unit. The examiner holds that the combined polynomials amount to the encryption algorithm. Schwan discloses executing an encryption algorithm in at least paragraph 0015 and therefore teaches the limitation implementing the combined polynomials in the programmable processor unit.

With respect to claims 3 and 8, the appellant argues that the prior art does not disclose "wherein an eraser member serving, in the event of an intrusion into the device, to erase the processor unit." The appellant argues that this does not teach erasing a controller or microprocessor in the event of an intrusion. The examiner disagrees and has interpreted processor unit as a computing device, incorporating both memory and a controller. The examiner holds that if the appellant meant processor they would not have included unit as mere surplusage. Therefore, giving weight to every word, the prior art does teach erasing a processor unit in the event of an intrusion.

Appellant's arguments with respect to claims 2, 4, 5, 7, 9, and 10 amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Christian LaForgia/

Primary Examiner, Art Unit 2439

Conferees:

Mike Simitoski

/Michael J Simitoski/

Primary Examiner, Art Unit 2439

Edan Orgad

/Edan Orgad/

Supervisory Patent Examiner, Art Unit 2439